# Simulation-Sound NIZK Proofs for a Practical Language and Constant Size Group Signatures

Jens Groth*

UCLA, Computer Science Department
3531A Boelter Hall
Los Angeles, CA 90095, USA
jg@cs.ucla.edu

**Abstract.** Non-interactive zero-knowledge proofs play an essential role in many cryptographic protocols. We suggest several NIZK proof systems based on prime order groups with a bilinear map. We obtain linear size proofs for relations among group elements without going through an expensive reduction to an NP-complete language such as Circuit Satisfiability. Security of all our constructions is based on the decisional linear assumption.
The NIZK proof system is quite general and has many applications such as digital signatures, verifiable encryption and group signatures. We focus on the latter and get the first group signature scheme satisfying the strong security definition of Bellare, Shi and Zhang [7] in the standard model without random oracles where each group signature consists only of a constant number of group elements.
We also suggest a simulation-sound NIZK proof of knowledge, which is much more efficient than previous constructions in the literature.
Caveat: The constants are large, and therefore our schemes are not practical. Nonetheless, we find it very interesting for the first time to have NIZK proofs and group signatures that except for a constant factor are optimal without using the random oracle model to argue security.

**Keywords:** Non-interactive zero-knowledge, simulation-sound extractability, group signatures, decisional linear assumption.

## 1 Introduction

A non-interactive proof system allows a prover to convince a verifier about the truth of a statement. Zero-knowledge captures the notion that the verifier learns no more from the proof than the truth of the statement. We refer to the full paper [28] for formal definitions of non-interactive zero-knowledge (NIZK) proofs. Our goal in this paper is to construct short efficient prover NIZK proofs for languages that come up in practice when constructing cryptographic protocols. As an example of the usefulness of these new techniques, we construct group signatures consisting of a constant number of group elements.

* Supported by NSF grant No. 0456717, and NSF Cybertrust grant.

### 1.1 Setup

We use two cyclic groups $\mathbb{G}, \mathbb{G}_1$ of order $p$, where $p$ is a prime. We make use of a bilinear map $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$. I.e., for all $u, v \in \mathbb{G}$ and $a, b \in \mathbb{Z}$ we have $e(u^a, v^b) = e(u, v)^{ab}$. We require that $e(g, g)$ is a generator of $\mathbb{G}_1$ if $g$ is a generator of $\mathbb{G}$. We also require that group operations, group membership, and the bilinear map be efficiently computable. Such groups have been widely used in cryptography in recent years.

Let $\mathcal{G}$ be an algorithm that takes a security parameter as input and outputs $(p, \mathbb{G}, \mathbb{G}_1, e, g)$ such that $p$ is prime, $\mathbb{G}, \mathbb{G}_1$ are descriptions of groups of order $p$, $e : \mathbb{G} \times \mathbb{G} \to \mathbb{G}_1$ is an admissible bilinear map as described above and $g$ is a random generator of $\mathbb{G}$.

We use the decisional linear assumption from Boneh, Boyen and Shacham [10].

**Definition 1 (Decisional Linear Assumption (DLIN)).** *We say the decisional linear assumption holds for the bilinear group generator $\mathcal{G}$ if for all non-uniform polynomial time adversaries $\mathcal{A}$ we have*

$$\begin{aligned} &\Pr\Big[(p, \mathbb{G}, \mathbb{G}_1, e, g) \leftarrow \mathcal{G}(1^k); x, y, r, s \leftarrow \mathbb{Z}_p : \\ &\qquad\qquad \mathcal{A}(p, \mathbb{G}, \mathbb{G}_1, e, g, g^x, g^y, g^{xr}, g^{ys}, g^{r+s}) = 1\Big] \\ \approx\ &\Pr\Big[(p, \mathbb{G}, \mathbb{G}_1, e, g) \leftarrow \mathcal{G}(1^k); x, y, r, s, d \leftarrow \mathbb{Z}_p : \\ &\qquad\qquad \mathcal{A}(p, \mathbb{G}, \mathbb{G}_1, e, g, g^x, g^y, g^{xr}, g^{ys}, g^{d}) = 1\Big]. \end{aligned}$$

Throughout the paper, we work over a bilinear group $(p, \mathbb{G}, \mathbb{G}_1, e, g) \leftarrow \mathcal{G}(1^k)$ generated such that the DLIN assumption holds for $\mathcal{G}$. We call this a DLIN group. Honest parties always check group membership of $\mathbb{G}, \mathbb{G}_1$ when relevant and halt if an element does not belong to a group that it was supposed to according to the protocol.

Given a DLIN group $(p, \mathbb{G}, \mathbb{G}_1, e, g)$ we can set up a semantically secure cryptosystem as in [10]. We choose at random $x, y \leftarrow \mathbb{Z}_p^*$. The public key is $(f, h)$, where $f = g^x, h = g^y$, and the secret key is $(x, y)$. To encrypt a message $m \in \mathbb{G}$ we choose $r, s \leftarrow \mathbb{Z}_p$ and let the ciphertext be $(u, v, w) = (f^r, h^s, g^{r+s}m)$. To decrypt a ciphertext $(u, v, w) \in \mathbb{G}^3$ we compute $m = D(u, v, w) = u^{-1/x}v^{-1/y}w$.

The cryptosystem $(K_{\mathrm{cpa}}, E, D)$ has several nice properties. The DLIN assumption for $\mathcal{G}$ implies semantic security under chosen plaintext attack (CPA). All triples $(u, v, w) \in \mathbb{G}^3$ are valid ciphertexts. Also, the cryptosystem is homomorphic.

$$E(m_1; r_1, s_1)E(m_2, r_2, s_2) = E(m_1m_2; r_1 + r_2, s_1 + s_2).$$

### 1.2 Pairing Product Equations

Given a group $(p, \mathbb{G}, \mathbb{G}_1, e, g)$ we define a pairing product equation of length $\ell$ over variables $a_1, \ldots, a_n$ to be an equation of the following form.

$$\prod_{j=1}^{\ell} e(q_{j,0}, q_{j,1}) = 1, \ \text{ where } \ q_{j,b} = b_{j,b} \prod_{i=1}^{n} a_i^{e_{j,b,i}} \ \text{ with } \ b_{j,b} \in \mathbb{G}\ ,\ e_{j,b,i} \in \mathbb{Z}_p.$$

Given a set $S$ of pairing product equations $\mathrm{eq}_1, \ldots, \mathrm{eq}_m$ we can ask the natural question: *Is there a tuple* $(a_1, \ldots, a_n) \in \mathbb{G}^n$ *such that all equations in* $S$ *are simultaneously satisfied?*

To illustrate the generality of the language of satisfiable pairing product equations we observe a reduction from the NP-complete language Circuit Satisfiability. Let $a_1, \ldots, a_n$ correspond to the wires of the circuit, which without loss of generality contains only NAND-gates. Let $S$ contain equations $e(a_i, a_i g^{-1}) = 1$ forcing each $a_i = g^{b_i}$ to encode a bit $b_i \in \{0, 1\}$. For each NAND-gate with input wires $i_0, i_1$ and output $i_2$ add to $S$ the equation $e(a_{i_0}, a_{i_1}) = e(g, g a_{i_2}^{-1})$, which is satisfied if and only if $b_{i_2} = \neg(b_{i_0} \wedge b_{i_1})$.

Our main motivation for being interested in satisfiability of pairing product equations is not NP-completeness though. Satisfiability of pairing product equations comes up in practice when constructing cryptographic protocols and by making a direct NIZK proof instead of first reducing the problem to some other language such as Circuit Satisfiability we keep proofs short.

For concreteness, let us use verifiable encryption as an example of a pairing product satisfiability question that may come up in practice. Suppose $(u, v, w)$ is a ciphertext under the public key $(f, h)$ of the DLIN-based cryptosystem described earlier. We are interested in whether this ciphertext encrypts a particular message $m$. This is the case, if and only if there exists $a$ such that $e(g, u) = e(a, f)$ and $e(h, wm^{-1}a^{-1})) = e(v, g)$. If we know $r, s$ we can compute the satisfiability witness $a = g^r$.

### 1.3 NIZK Proofs for Satisfiability of Pairing Product Equations

NIZK PROOFS. The central technical contribution of this paper is an NIZK proof of size $\mathcal{O}(n + \ell)$ group elements for satisfiability of a set of pairing product equations of combined length $\ell = \sum_{j=1}^{m} \ell_j$. The proof system has perfect completeness and perfect soundness.

RELATED WORK ON NIZK PROOFS. NIZK proofs were introduced by Blum, Feldman and Micali [9] and they suggested an NIZK proof for a single statement based on the hardness of deciding quadratic residousity. Blum et al. [8] extended this to multi-theorem NIZK proofs. Feige, Lapidot and Shamir [25] and Kilian and Petrank [33] give constructions based on trapdoor permutations.

Recently Groth, Ostrovsky and Sahai [30] have constructed NIZK proofs from composite order bilinear groups introduced by Boneh, Goh and Nissim [11]. Even more recently Groth, Ostrovsky and Sahai [29] have introduced the setting in this paper, a bilinear group of prime order and the DLIN assumption. They construct non-interactive witness-indistinguishable proofs without any setup assumptions. In the common reference string (CRS) model both results give NIZK proofs for Circuit Satisfiability of size $\mathcal{O}(|C|)$ group elements.

All the above-mentioned papers have in common that they focus on an NP-complete language, usually Circuit Satisfiability, and suggest a bit-by-bit or gate-by-gate NIZK proof for this language. Our paper differs by introducing new techniques that allows making *direct* NIZK proofs for satisfiability of pairing product equations. This allows us to construct constant/linear size cryptographic protocols for digital signatures, RCCA-secure encryption[20], verifiable encryption and group signatures.

The only other way we know of to get linear size NIZK proofs/arguments for any practical language is the Fiat-Shamir heuristic: Make a 3-move public coin (honest verifier) zero-knowledge protocol non-interactive by computing the verifier's challenge as a hash of the statement and the initial protocol message. To argue security, one models the hash-function as a random oracle [6]. It is well known that using the random oracle model sometimes results in insecure real life protocols [18, 19, 34, 27, 4]. In comparison, our NIZK proofs have *provable security* under the DLIN assumption.

SIMULATION-SOUND EXTRACTABLE NIZK PROOFS. Combining the definitions of simulation-soundness introduced by Sahai [35] and proofs of knowledge from De Santis and Persiano [23], we get simulation-sound extractability. Here the simulator first creates a simulated CRS together with a simulation trapdoor and an extraction trapdoor. We require that even after the adversary has seen simulated proofs on arbitrary statements, if it constructs a new valid proof on any statement, then we can extract a witness. Simulation-sound extractability is a very strong notion, in particular it implies non-malleability as defined by De Santis et al. [22].

We construct a simulation-sound extractable NIZK proof for satisfiability of pairing product equations. Our NIZK proof has a CRS with a description of the group and a constant number of group elements, and the proofs consist of $\mathcal{O}(n+\ell)$ group elements.

RELATED WORK ON SIMULATION-SOUND NIZK PROOFS. As stated before, our interest in this paper is satisfiability of pairing products equations. However, in order to compare our scheme with previous work let us look at the case of Circuit Satisfiability. [35] constructed a one-time simulation-sound NIZK proof system using techniques from Dwork, Dolev and Naor [24]. Later a construction for unbounded simulation-sound extractable NIZK arguments was given by [22], where the adversary can see many simulated arguments of arbitrary statements. The schemes from both these papers are based on trapdoor permutations but are not practical. For the sake of fairness in evaluating the quality of our contribution, we have also considered whether the techniques from [30] could be used to get good efficiency for simulation-sound extractability. The answer to this question seems to be negative, the best construction we can think of using GOS-techniques gives an additive polynomial size overhead.

| Scheme | NIZK proof bit size | Assumption |
|---|---|---|
| [22] | $\mathcal{O}(\|C\|\mathrm{poly}(k))$ | Trapdoor permutations |
| Potential use of [30] techniques | $\mathcal{O}(\|C\|k+\mathrm{poly}(k))$ | Subgroup decision |
| This paper | $\mathcal{O}(\|C\|k)$ | DLIN |

**Fig. 1.** Comparison of simulation-sound extractable proofs for Circuit Satisfiability

COMMON REFERENCE STRING VERSUS UNIFORM RANDOM STRING. We will construct NIZK proofs and simulation-sound extractable NIZK proofs in the common reference string model, where the prover and the verifier both have access to a CRS chosen according to some distribution. If this distribution is uniform at random we call it the uniform random string model. In some settings it is easier to work with a URS, for instance a URS can easily be jointly generated using multi-party computation techniques.

Our NIZK proofs use a common reference string that contains a description of a bilinear group and a number of group elements. Depending on the group elements, the CRS will give either perfect soundness of perfect zero-knowledge. With overwhelming probability random group elements will lead to a perfect soundness CRS. Assuming that we can use a uniform random string to get a description of a DLIN group and a number of random group elements, we will therefore get NIZK proofs and simulation-sound NIZK proofs in the URS-model. Since there is a negligible chance of picking a perfect zero-knowledge CRS, this gives statistical soundness instead of perfect soundness, which is the best we can hope for in the URS-model. We remark that natural candidates for bilinear DLIN groups based on elliptic curves are efficiently samplable from a URS [29]. For the sake of simplicity we will just work with the CRS-model in the paper, but invite the reader to note that all constructions work in the URS-model as well.

### 1.4 An Application: Constant Size Group Signatures

Group signatures, introduced by Chaum and van Heyst [21], allow a member to sign messages anonymously on behalf of a group. A group manager controls the group and decides who can join. In case of abuse, the group manager is able to open a signature to reveal who the signer is. It is hard to design group signatures and most schemes [17, 16, 3, 14, 2, 13, 31, 15, 10, 26, 32] use the random oracle model in the security proof.

Bellare, Micciancio and Warinschi [5] suggest rigorous security definitions for group signatures in the *static* case where the set of members is fixed from the start and never changes. Bellare, Shi and Zhang [7] extend the security model to the partially *dynamic* case where the group manager can enroll new members in the group. Both [5] and [7] suggest constructions of group signatures based on trapdoor permutations. These constructions are very inefficient and only indicate feasability.

Boyen and Waters [12] use a combination of the Waters signature scheme [36] and the [30] NIZK proofs. They assume a static setting and as part of a group signature they encrypt the identity of the signer bit by bit. This means that a group signature consists of $\mathcal{O}(\log n)$ group elements, where $n$ is the number of members in the group. The group signature scheme satisfies a relaxed version of the [5] security definition, where the anonymity is guaranteed only when no signatures have been opened and traced to the signer. In comparison, the full-anonymity definition in [5] demands that anonymity is preserved even when the adversary can get an opening of any other signature than the challenge.

Ateniese et al. [1] use a bilinear group of prime order. The advantage of this scheme is that it is very efficient, a group signature consists of 8 group elements. However, they use several strong security assumptions and their security model is even weaker than that of [12] since it does not protect against key-exposures; knowledge of a signing key immediately allows one to tell which signatures this member has made. In comparison, the BMW,BSZ-models do guard against key exposure.

The tools in this paper give a construction of group signatures where both keys and signatures consist of a constant number of group elements. The construction involves carefully constructing and tailoring a signature scheme and the simulation-sound extractable NIZK proof system such that they fit each other. The constant is large; we do not claim this to be a practical scheme. Rather this should be seen as an interesting feasibility result; under a simple and natural security assumption there exists an up to a constant optimal dynamic group signature scheme satisfying the strong security definitions from [5, 7].

| Scheme | Signature in bits | Security model | Assumption |
|---|---|---|---|
| [5] | $\mathrm{poly}(k)$ | BMW [5] (fixed group) | Trapdoor permutations |
| [7] | $\mathrm{poly}(k)$ | BSZ [7] (dynamic group) | Trapdoor permutations |
| [12] | $3k + 2k \log n$ | BMW [5], CPA-anonymity | Subgroup decision and CDH |
| [1] | $8k$ | UC-model, non-adaptive adv. | Strong SXDH, q-EDH, strong LRSW |
| This paper | $\mathcal{O}(k)$ | BSZ [7] | DLIN |

**Fig. 2.** Comparison of group signature schemes

# 2 Preliminaries

## 2.1 Definitions: Non-interactive Zero-Knowledge Proofs

We provide formal definitions of non-interactive proofs, perfect completeness, perfect soundness, unbounded adaptive zero-knowledge, composable zero-knowledge, perfect proofs of knowledge, simulation soundness and simulation-sound extractability in the full paper. Here we will just sketch one useful stronger definition of zero-knowledge that we have not seen elsewhere in the literature.

COMPOSABLE ZERO-KNOWLEDGE. We define composable zero-knowledge by making two requirements. First, a real CRS is computationally indistinguishable from a simulated CRS; we call this reference string indistinguishability. Second, the adversary *even when it gets access to the simulation trapdoor* $\tau$, cannot distinguish real proofs on the simulated CRS from simulated proofs. We call this simulation indistinguishability. We refer to the full paper for the formal definition and a proof that composable zero-knowledge implies the standard notion of unbounded adaptive zero-knowledge usually found in the literature.

Our motivation for introducing the notion of composable zero-knowledge is that it allows different zero-knowledge proofs for *different* languages to use the *same* CRS. Suppose we have relations $R_1, \ldots, R_n$ and corresponding NIZK proof systems $(K, P_1, V_1), \ldots, (K, P_n, V_n)$ with composable zero-knowledge using the same key generator and CRS simulator $K, S_1$. A hybrid argument shows that no non-uniform polynomial time adversary can distinguish real proofs on a simulated CRS from simulated proofs on this CRS for relation $R_i$, *even if it sees arbitrary proofs or simulations for statements in* $L_{j \neq i}$ *using the same CRS*. The reason is that in the definition of simulation indistinguishability we give $\tau$ to the adversary, so it can itself implement the simulator $S_{2,j}$ for any relation $R_{j \neq i}$.

Composable zero-knowledge implies that the zero-knowledge property still makes sense when many different NIZK proofs use the same CRS. In our paper, all the NIZK proofs will indeed generate the CRS in the same way and simulate the CRS in the same way, so we get better performance by not having to deal with different CRSs for each proof system. At the same time, it simplifies the paper.

### 2.2 A Homomorphic Commitment Scheme

We use the cryptosystem from Section 1.1 to create a homomorphic commitment scheme such that depending on how we generate the public key we get either a perfectly binding commitment scheme or a perfectly hiding trapdoor commitment scheme. The idea is that if $K$ is an encryption of 1, then $K^m E(1; r, s)$ is also an encryption of 1 and we have a perfectly hiding commitment to $m$. On the other hand, if $K$ is not an encryption of 1, then $K^m E(1; r, s)$ is perfectly binding.

**Perfectly binding key generation:** Let $ck = (p, \mathbb{G}, \mathbb{G}_1, e, g, f, h, u, v, w)$ where $f, h$ is a public key for the cryptosystem and $(u, v, w) = (f^{r_u}, h^{s_v}, g^{t_w})$ with $t_w \neq r_u + s_v$ is an encryption of a non-trivial element.

**Perfectly hiding trapdoor key generation:** Let $ck = (p, \mathbb{G}, \mathbb{G}_1, e, g, f, h, u, v, w)$ where $f, h$ is a public key for the cryptosystem and $(u, v, w) = (f^{r_u}, h^{s_v}, g^{r_u+s_v})$ is an encryption of 1.
The corresponding trapdoor key is $tk = (ck, x, y, r_u, s_v)$.

**Commitment:** To commit to message $m \in \mathbb{Z}_p$ pick $r, s \leftarrow \mathbb{Z}_p$ and let the commitment be $c = (c_1, c_2, c_3) = \mathrm{com}(m; r, s) = (u^m f^r, v^m h^s, w^m g^{r+s})$.

The commitment schemes $(K_{\mathrm{binding}}, \mathrm{com})$ and $(K_{\mathrm{hiding}}, \mathrm{com})$ have several nice properties. The CPA-security of the cryptosystem implies that one cannot distinguish perfect binding keys from perfect hiding keys. This in turn implies computational hiding respectively computational binding for the two schemes. The homomorphic property of the cryptosystem transfers to the commitment scheme.

$$\mathrm{com}(m_1 + m_2; r_1 + r_2, s_1 + s_2) = \mathrm{com}(m_1; r_1, s_1)\mathrm{com}(m_2; r_2, s_2).$$

For the perfectly binding commitment scheme, any $c \in \mathbb{G}^3$ is a commitment to some message $m \in \mathbb{Z}_p$.

## 3 Efficient Non-interactive Zero-Knowledge Proof Systems

The construction of our NIZK proof for satisfiability of pairing product equations is very complex and requires many new techniques. We will therefore build it in a modular fashion from NIZK proofs for simpler relations. Even some of these simpler NIZK proofs are complex and we can only sketch the ideas behind the constructions here. The full paper [28] contains full constructions and security proofs.

### 3.1 Common Reference String

All the NIZK proofs in this section use the same CRS generator $K$ and CRS simulator $S_1$ described below. A CRS is a public key for the perfectly binding commitment scheme described in the previous section. The soundness of the NIZK proofs comes from the perfect binding property of the commitment scheme, which makes it impossible for any adversary to cheat. In simulations, we use a public key for the perfectly hiding commitment scheme as the simulated CRS.

**Common reference string:**
Generate $\sigma = (p, \mathbb{G}, \mathbb{G}_1, e, g, f, h, u, v, w) \leftarrow K_{\text{binding}}(1^k)$.[1]
**Simulated reference string:**
Generate $(\sigma, \tau) \leftarrow K_{\text{hiding}}(1^k)$, where $\sigma = (p, \mathbb{G}, \mathbb{G}_1, e, g, f, h, u, v, w)$ and $\tau = (x, y, r_u, s_u)$.

The CPA-security of the cryptosystem gives us the following lemma.

**Lemma 1.** *If $(p, \mathbb{G}, \mathbb{G}_1, e, g)$ is a DLIN group, then $(K, S_1)$ has reference string indistinguishability.*

### 3.2 NIZK Proofs for Commitment to 0

Let $R_{\text{zero}} = \{(c, (r, s)) \mid c = \text{com}(0; r, s)\}$ define the language of commitments to 0. The proof of the following theorem can be found in the full paper.

**Theorem 1.** *There exists an NIZK proof system $(K, P_{\text{zero}}, V_{\text{zero}}, S_1, S_{\text{zero}})$ for $R_{\text{zero}}$ with perfect completeness, perfect soundness and composable zero-knowledge with perfect simulation indistinguishability under the DLIN assumption for $\mathcal{G}$. The proof consists of 1 group element ($\pi = g^r$). Verification corresponds to evaluating two pairing product equations.*

### 3.3 Proof for Committed Multiplicative Relationship

Consider three commitments $c_a, c_b, c_c$ such that the corresponding messages have a multiplicative relationship $m_c = m_a m_b$. The corresponding relation is $R_{\text{mult}} = \{((c_a, c_b, c_c), (m_a, r_a, s_a, m_b, r_b, s_b, r_c, s_c)) \mid c_a = \text{com}(m_a; r_a, s_a), c_b = \text{com}(m_b; r_b, s_b), c_c = \text{com}(m_a m_b; r_c, s_c)\}$.

**Theorem 2.** *There exists an NIZK proof $(K, P_{\text{mult}}, V_{\text{mult}}, S_1, S_{\text{mult}})$ for $R_{\text{mult}}$ with perfect completeness, perfect soundness and composable zero-knowledge if the DLIN assumption holds for $\mathcal{G}$. A proof consists of 36 group elements. Verification corresponds to evaluating a set of pairing product equations.*

*Sketch of proof.* $c_a, c_b, c_c$ have a multiplicative relationship if and only if

$$c_c = c_b^{m_a} \text{com}(0; r_c - m_a r_b, s_c - m_a s_b).$$

[1] Both the CRS generator $K$ and the CRS simulator $S_1$ first create a DLIN group honestly. This means that instead of generating the CRSs from scratch, it is also possible to build any of the NIZK proofs we construct in the following sections on top of an already existing DLIN group. When doing so we write $\sigma \leftarrow K(p, \mathbb{G}, \mathbb{G}_1, e, g)$ or $(\sigma, \tau) \leftarrow S_1(p, \mathbb{G}, \mathbb{G}_1, e, g)$.

To prove the latter, it suffices to reveal $m_a$, and prove that $c_a\mathrm{com}(-m_a;0,0)$ and $c_c c_b^{-m_a}$ are commitments to 0. To get zero-knowledge, we tweak this idea in a way such that $m_a$ is not revealed directly.

The main trick in the NIZK proof is to pick exponents $r, s$ at random, which will be used to hide $m_a$. Using $(K, P_{\text{zero}}, V_{\text{zero}})$ we prove that

$$\begin{aligned} & c_a\mathrm{com}(1;0,0)^{-(r+s+m_a)}(\mathrm{com}(1;0,0)\pi_{0,1})^r(\mathrm{com}(1;0,0)\pi_{0,3})^s \\ \text{and} \quad & c_c c_b^{-(r+s+m_a)}(c_b\pi_{0,2})^r(c_b\pi_{0,4})^s \end{aligned}$$

are commitments to 0, where $\pi_{0,1}, \pi_{0,2}, \pi_{0,3}, \pi_{0,4}$ are themselves commitments to 0.

Revealing the components $\mathrm{com}(1;0,0)^{r+s+m_a}, c_b^{r+s+m_a}$, the verifier can use the bilinear maps to check that there exists some common exponent $t = r + s + m_a$, even though it cannot compute the exponent itself. Similarly, revealing $(\mathrm{com}(1;0,0)\pi_{0,1})^r, (c_b\pi_{0,2})^r$ and $(\mathrm{com}(1;0,0)\pi_{0,3})^s, (c_b\pi_{0,4})^s$ allows the verifier to check that there exist common exponents $r, s$.

We are verifiably using the same exponents $r, s, t$ on $\mathrm{com}(1;0,0)$ and $c_b$ to get respectively $c_a$ and $c_c$. This shows that

$$c_a\mathrm{com}(1;0,0)^{r+s-t} \quad \text{and} \quad c_c c_b^{r+s-t}$$

are both commitments to 0. The only way this can be possible is when $m_a = t - r - s$.

Computational simulation indistinguishability follows from the fact that while we use the same exponents, we use different bases. Therefore, at no point is any element itself raised to $m_a$, which the adversary could potentially use to detect whether it was a correct proof or one created by a simulator, which does not know $m_a$. The commitments $\pi_{0,1}, \pi_{0,2}, \pi_{0,3}, \pi_{0,4}$ rerandomize the bases that we raise to $r, s$ and therefore $t = r + s + m_a$ is indistinguishable from $t$ random, so $m_a$ is hidden. □

### 3.4 NIZK Proof for Commitment to Exponent

We have two elements $a, b$ and a commitment $c$ to the exponent $m$ so $b = a^m$. $R_{\text{expo}} = \{((a,b,c),(m,r,s)) \mid b = a^m, c = \mathrm{com}(m;r,s)\}$ defines the language of such statements.

**Theorem 3.** *There exists an NIZK proof $(K, P_{\text{expo}}, V_{\text{expo}}, S_1, S_{\text{expo}})$ for $R_{\text{expo}}$ with perfect completeness, perfect soundness and composable zero-knowledge with perfect simulation indistinguishability if the DLIN assumption holds for $\mathcal{G}$. A proof consists of 8 group elements. Verification consists of evaluating a set of pairing product equations.*

*Sketch of proof.* If $a \neq 1$ then one can use the bilinear map to verify that a pair of commitments $\pi_1, \pi_m$ have the same exponent $m$ so $\pi_m = \pi_1^m$. If $\pi_1$ is a commitment to 1, then $\pi_m$ is a commitment to $m$. What remains is to prove that $\pi_1\mathrm{com}(-1;0,0)$ and $c_m\pi_m^{-1}$ are commitments to 0, which we can do with the NIZK proof for commitment to 0.

To prove zero-knowledge we observe that on a perfect hiding key $ck$

$$\pi_1 = (a^{xr_1}, a^{ys_1}, a^{r_1+s_1}) \quad \text{and} \quad \pi_m = (b^{xr_1}, b^{ys_1}, b^{r_1+s_1})$$

gives us commitments so $\pi_m = \pi_1^m$, even though we do not know $m$ itself. □

### 3.5 NIZK Proof for Generalized Pedersen Commitment

Consider a Pedersen commitment to many messages $b = g^t \prod_{i=1}^n a_i^{m_i}$. Let $c_t, c_1, \ldots, c_n$ be commitments to the exponents. The language of multi-message Pedersen commitments and corresponding exponent-commitments is defined by $R_{\text{m-ped}} = \{((a_1, \ldots, a_n, b, c_t, c_1, \ldots, c_n), (t, r_t, s_t, m_1, r_1, s_1, \ldots, m_n, r_n, s_n)) \mid b = g^t \prod_{i=1}^n a_i^{m_i}, c_t = \text{com}(t; r_t, s_t), c_i = \text{com}(m_i, r_i, s_i)\}$.

**Theorem 4.** *There exists an NIZK proof* $(K, P_{\text{m-ped}}, V_{\text{m-ped}}, S_1, S_{\text{m-ped}})$ *for* $R_{\text{m-ped}}$ *with perfect completeness, perfect soundness and composable zero-knowledge if the DLIN assumption holds for* $\mathcal{G}$*. The proof consists of* $63n - 4$ *group elements. The verification consists of evaluating a set of pairing product equations.*

*Sketch of Proof.* The hard part in constructing an NIZK proof for $R_{\text{m-ped}}$ is to construct a proof for the one-message Pedersen commitment relation $R_{\text{ped}}$, which is done with techniques related to the NIZK proof for multiplicative relationship, see the full paper for details. Once we have that, we split $b$ into $n$ one-message Pedersen commitments $b = \prod_{i=1}^n b_i = \prod_{i=1}^n (a_i^{m_i} g^{t_i})$ choosing the $t_i$'s at random so $t = \sum_{i=1}^n t_i$ and make commitments $c_{t_i}$ to the $t_i$'s. We make an NIZK proof for $R_{\text{ped}}$ for each of the statements $(a_i, b_i, c_i, c_{t_i})$. □

### 3.6 NIZK Proof for Committed Bilinear Product

We can commit to $a_1, b_1, \ldots, a_n, b_n$ in the following way. We form $A_i = g^{r_i} a_i$ and commitments $c_{r_i}$ to $r_i$. Similarly, we form $B_i = g^{s_i} b_i$ and commitments $c_{s_i}$ to $s_i$. We are interested in knowing whether $\prod_{i=1}^n e(a_i, b_i) = 1$.

Let $R_{\text{bil-prod}} = \{(A_1, c_{r_1}, B_1, c_{s_1}, \ldots, A_n, c_{r_n}, B_n, c_{s_n}), (r_1, r_{r_1}, s_{r_1}, s_1, r_{s_1}, s_{s_1}, \ldots, r_n, r_{r_n}, s_{r_n}, s_n, r_{s_n}, s_{s_n}) \mid A_i = g^{r_i} a_i, B_i = g^{s_i} b_i, c_{r_i} = \text{com}(r_i; r_{r_i}, s_{r_i}), c_{s_i} = \text{com}(s_i; r_{s_i}, s_{s_i}), \prod_{i=1}^n e(a_i, b_i) = 1\}$.

**Theorem 5.** *There exists an NIZK proof* $(K, P_{\text{bil-prod}}, V_{\text{bil-prod}}, S_1, S_{\text{bil-prod}})$ *for* $R_{\text{bil-prod}}$ *with perfect completeness, perfect soundness and composable zero-knowledge under the DLIN assumption for* $\mathcal{G}$*. Proofs consist of* $228n-3$ *group elements and verification corresponds to evaluating a set of pairing product equations.*

*Sketch of proof.* The key observation in the construction is that if and only if $\prod_{i=1}^n e(a_i, b_i) = 1$. we have for arbitrary $R_1, S_1, \ldots, R_n, S_n \in \mathbb{Z}_p$ that

$$\begin{aligned}
\prod_{i=1}^n e(A_i, B_i) &= \prod_{i=1}^n e(g^{r_i}, g^{s_i} b_i) e(g^{r_i} a_i, g^{s_i}) e(g^{r_i}, g^{s_i})^{-1} \prod_{i=1}^n e(a_i, b_i) \\
&= \prod_{i=1}^n e(g, B_i)^{r_i} e(A_i, g)^{s_i} e(g, g)^{-r_i s_i} = e(g, g^{-\sum_{i=1}^n r_i s_i} \prod_{i=1}^n A_i^{s_i} B_i^{r_i}) \\
&= e(g, g^{-\sum_{i=1}^n (r_i s_i + R_i S_i)} \prod_{i=1}^n A_i^{s_i} B_i^{r_i}) \prod_{i=1}^n e(g^{R_i}, g^{S_i}).
\end{aligned}$$

In the NIZK proof, we pick $R_1, S_1, \ldots, R_n, S_n$ at random. We commit to $R_i, S_i$ and we already have commitments to $r_i, s_i$. We reveal the $2n + 1$ elements $g^{R_1}, g^{S_1}, \ldots, g^{R_n}, g^{S_n}$ and $g^{-\sum_{i=1}^n (r_i s_i + R_i S_i)} \prod_{i=1}^n A_i^{s_i} B_i^{r_i}$. We then use NIZK proofs for $R_{\mathrm{expo}}, R_{\mathrm{mult}}, R_{\mathrm{m-ped}}$ to prove that they have been formed correctly.

In the simulation, we observe that for arbitrary $R_1, S_1, \ldots, R_n, S_n$

$$\prod_{i=1}^n e(A_i, B_i) = e(g, g^{-\sum_{i=1}^n R_i S_i} \prod_{i=1}^n A_i^{-S_i} B_i^{-R_i}) \prod_{i=1}^n e(g^{R_i} A_i, g^{S_i} B_i).$$

Picking $R_1, S_1, \ldots, R_n, S_n$ randomly means all elements have the same distribution as in a real proof on a simulated CRS. We can then simulate the NIZK proofs for $R_{\mathrm{expo}}, R_{\mathrm{mult}}, R_{\mathrm{m-ped}}$. □

### 3.7 NIZK Proof for Satisfiability of Pairing Product Equations

Recall from the introduction that a pairing product equation is of the form

$$\mathrm{eq}(a_1, \ldots, a_n) : \prod_{j=1}^{\ell} e(q_{j,0}, q_{j,1}) = 1 \text{ , where } q_{j,b} = b_{j,b} \prod_{i=1}^n a_i^{e_{j,b,i}},$$

for known $b_{j,b} \in \mathbb{G}$ and $e_{j,b,i} \in \mathbb{Z}_p$. A set $S$ of pairing product equations $\mathrm{eq}_1, \ldots, \mathrm{eq}_m$ is said to be satisfiable if there exists $(a_1, \ldots, a_n) \in \mathbb{G}^n$ such that all equations are satisfied. Let $R_{\mathrm{ppsat}} = \{ S \mid \exists (a_1, \ldots, a_n) \in \mathbb{G}^n \; \forall eq_k \in S : eq_k(a_1, \ldots, a_n) = \mathtt{true} \}$. We conclude this section with the following main theorem.

**Theorem 6.** *There exists an NIZK proof $(K, P_{\mathrm{ppsat}}, V_{\mathrm{ppsat}}, S_1, S_{\mathrm{ppsat}})$ for $R_{\mathrm{ppsat}}$ with perfect completeness, perfect soundness and composable zero-knowledge if the DLIN assumption holds for $\mathcal{G}$. Proofs consist of $4n + 228\ell - 3m$ group elements, where $\ell = \sum_{k=1}^m \ell_k$. Verification consists of evaluating a set of pairing product equations.*

*Sketch of proof.* In the NIZK proof, we first commit to each $a_i$ as $g^{t_i} a_i$ and $\mathrm{com}(t_i)$. Using homomorphic properties, it is straightforward for $q_{k,j,b}$ in equation $eq_k$ to compute $g^{t_{k,j,b}} q_{k,j,b}$ and $\mathrm{com}(t_{k,j,b})$ as

$$b_{k,j,b} \prod_{i=1}^n (g^{t_i} a_i)^{e_{k,j,b,i}} = g^{\sum_{i=1}^n t_i e_{k,j,b,i}} (b_{k,j,b} \prod_{i=1}^n a_i^{e_{k,j,b,i}})$$

$$\text{and} \quad \prod_{i=1}^n \mathrm{com}(t_i)^{e_{k,j,b,i}} = \mathrm{com}(\sum_{i=1}^n t_i e_{k,j,b,i}).$$

For each pairing product equation $\mathrm{eq}_k$ make an NIZK proof for $R_{\mathrm{bil-prod}}$ that $\prod_{j=1}^{\ell_k} e(q_{k,j,0}, q_{k,j,1}) = 1$. □

NESTING NIZK PROOFS. Since verification consists of verifying a set of pairing product equations, we can nest NIZK proofs inside one another. I.e., we can prove that there exists an NIZK proof such that there exists an NIZK proof such that, etc. Each level of nesting costs a constant blow-up factor. In comparison, this is very expensive with other NIZK proofs and impossible in the random oracle model.

REDUCING THE NUMBER OF VARIABLES. Consider a set of pairing product equations over $n$ variables with combined length $\ell$. We show in the full paper that there is a set of pairing product equations of length $\ell$ over $n' \leq 2\ell$ variables, such that this set is satisfiable if and only if the original set is satisfiable. This gives us NIZK proofs of length $\mathcal{O}(\ell)$ group elements for satisfiability of pairing product equations.

## 4 Simulation-Sound Extractable NIZK Proof for Satisfiability of Pairing Product Equations

A CMA-SECURE SIGNATURE SCHEME. With the help of the NIZK proof for $R_{\mathrm{ppsat}}$, we can construct a digital signature scheme secure against adaptive chosen message attack (CMA).

**Theorem 7.** *Under the DLIN assumption there exists a CMA-secure digital signature scheme* $(K_{\mathrm{sign}}, \mathrm{Sign}, \mathrm{Ver})$ *for signing* $n$ *group elements with perfect correctness. The verification key and the signatures consist of* $\mathcal{O}(n)$ *group elements and the verification process consists of evaluating a set of pairing product equations.*

Due to lack of space we refer the reader to the full paper [28] for the construction and the proof. We remark on one issue that makes the construction non-trivial. Our NIZK proofs work for pairing product equations. Since we want to use the NIZK proofs on encrypted signatures, we cannot use a hash-function in the signature scheme, since we do not know how to make NIZK proofs for correct hashing without an expensive NP-reduction to e.g. Circuit Satisfiability.

SIMULATION-SOUND EXTRACTABLE NIZK PROOFS. We will combine the CMA-secure signature scheme with the NIZK proofs to construct an unbounded simulation-sound extractable NIZK proof for $R_{\mathrm{ppsat}}$.

**Common reference string and simulated reference string:** Given a group $(p, \mathbb{G}, \mathbb{G}_1, e, g)$ pick CMA-secure signature keys $(vk, sk) \leftarrow K_{\mathrm{sign}}(p, \mathbb{G}, \mathbb{G}_1, e, g)$, keys for the CPA-secure cryptosystem $(pk, sk_{\mathrm{cpa}}) \leftarrow K_{\mathrm{cpa}}(p, \mathbb{G}, \mathbb{G}_1, e, g)$ and make a ciphertext $c_1 \leftarrow E_{pk}(t)$ for $t \neq 1$. Let $\sigma \leftarrow K(p, \mathbb{G}, \mathbb{G}_1, e, g)$ be a CRS for our NIZK proofs.
The CRS is $\Sigma = (vk, pk, c_1, \sigma)$.
In the simulation we pick $c_1 = E_{pk}(1; r_c, s_c)$ and let the simulation trapdoor be $\tau = (sk, r_c, s_c)$ while the extraction key is $\xi = sk_{\mathrm{cpa}}$.

**Proof:** Given a set of pairing product equations $S$ and a satisfiability witness $w = (a_1, \ldots, a_n)$ the proof is constructed as follows.
Pick keys $(vk_{\mathrm{sots}}, sk_{\mathrm{sots}})$ for a strong one-time signature scheme.[2] Encrypt $c_w \leftarrow E_{pk}(a_1, \ldots, a_n)$ and $c_s = E_{pk}(1, \ldots, 1)$. Make an NIZK proof $\pi_{\mathrm{ssor}}$ of the following statement: Either $c_w$ contains a satisfying witness, or $c_1$ contains 1 and $c_s$ contains a signature under $vk$ on $vk_{\mathrm{sots}}$. We refer to the full paper how to use the NIZK proof for $R_{\mathrm{ppsat}}$ to prove satisfiability of at least one out of two sets of pairing product equations. Finally, sign everything $s_{\mathrm{sots}} \leftarrow \mathrm{Sign}_{sk_{\mathrm{sots}}}(S, c_w, c_s, \pi_{\mathrm{ssor}})$.
The proof is $\pi = (vk_{\mathrm{sots}}, c_w, c_s, \pi_{\mathrm{ssor}}, s_{\mathrm{sots}})$.

[2] See the full paper for a DLIN group based strong one-time signature scheme.

**Simulation:** Pick keys $(vk_{\mathrm{sots}}, sk_{\mathrm{sots}})$ for a strong one-time signature scheme. Sign $vk_{\mathrm{sots}}$ as $s \leftarrow \mathrm{Sign}_{sk}(vk_{\mathrm{sots}})$. Encrypt $c_w \leftarrow E_{pk}(1,\ldots,1)$ and $c_s = E_{pk}(s)$. Make an NIZK proof $\pi_{\mathrm{ssor}}$ of the following statement: Either $c_w$ contains a satisfying witness, or $c_1$ contains 1 and $c_s$ contains a signature under $vk$ on $vk_{\mathrm{sots}}$. Finally, sign everything $s_{\mathrm{sots}} \leftarrow \mathrm{Sign}_{sk_{\mathrm{sots}}}(S, c_w, c_s, \pi_{\mathrm{ssor}})$.

**Verification and extraction:** Accept the proof if and only if the strong one-time signature $s_{\mathrm{sots}}$ and the proof $\pi_{\mathrm{ssor}}$ are valid.
To extract a witness simply decrypt $c_w$.

**Theorem 8.** *If $(p, \mathbb{G}, \mathbb{G}_1, e, g)$ is a DLIN group then $(K_{\mathrm{sse}}, P_{\mathrm{sse}}, V_{\mathrm{sse}}, S_{1,\mathrm{sse}}, S_{\mathrm{sse}}, E_{1,\mathrm{sse}}, E_{\mathrm{sse}}, SE_{1,\mathrm{sse}})$ is an NIZK proof for $R_{\mathrm{ppsat}}$ with perfect completeness, perfect soundness, perfect knowledge extraction and composable zero-knowledge and unbounded simulation-sound extractability. The size of the CRS is $\mathcal{O}(1)$ group elements, while the NIZK proofs consist of $\mathcal{O}(n+\ell)$ group elements.*

*Sketch of proof.* On a real CRS, $c_1$ does not contain 1, and therefore by the perfect soundness of the NIZK proof $c_w$ must contain a satisfiability witness $w$. In simulations, $c_1$ does contain 1, however, since the prover does not know the signing key $sk$ he cannot create signatures on $vk_{\mathrm{sots}}$ of his own choosing and he cannot recycle a $vk_{\mathrm{sots}}$ either because he does not know the corresponding signing key $sk_{\mathrm{sots}}$. Therefore, he cannot encrypt a signature in $c_s$, so he must still encrypt a satisfiability witness in $c_w$. We can then decrypt $c_w$ and extract the witness. We refer to the full paper for details. □

## 5 Constant Size Group Signatures without Random Oracles

SECURITY DEFINITIONS. [7] define three security properties that a group signature must satisfy: anonymity, traceability and non-frameability. We refer to the full paper for formal definitions and to [7] for a discussion of why this is a strong security definition that incorporates previous security requirements found in the literature. The definition allows for separating the roles of the group manager into an issuer who can enroll members and an opener that can open signatures to see who created it.

**Anonymity:** Only the opener can see who created a signature. This property must hold even if the members' keys are exposed and the issuer is corrupt.

**Traceability:** If the issuer is honest then all signatures will be correctly opened to some member.

**Non-frameability:** Even if the issuer and opener are both corrupt, they still cannot create a valid signature and a convincing opening that frames an honest member that did not sign it.

A GROUP SIGNATURE SCHEME. We imagine that there is a PKI in place so we have authenticated public keys. We model this by having a public key registry $reg$ where only user $i$ has one-time write access to $reg[i]$, we do not attempt to keep this information secret. User $i$ stores his secret key in $gsk[i]$, unless compromised only the user has access to this key.

**Key generation:** We create the group public key $gpk = (vk, pk, \Sigma)$, where $vk$ is a verification key for the CMA-secure signature scheme, $pk$ is a public key for the CPA-secure cryptosystem and $\Sigma$ is a CRS for the simulation-sound extractable NIZK proof. The issuer's key $ik$ is the signing key for the signature scheme, while the opener's key $ok$ is the decryption key for the cryptosystem.

**Join/Issue:** The user $i$ registers a public key $vk_i$ for the CMA-secure signature scheme in $reg[i]$ and stores the corresponding secret key $sk_i$. The issuer signs it as $cert_i \leftarrow \mathrm{Sign}_{ik}(vk_i)$. The user verifies the correctness of the signature and stores $gsk[i] = (sk_i, vk_i, cert_i)$.

**Sign:** To sign $m \in \{0,1\}^*$, member $i$ creates a strong one-time signature key pair $(vk_{\mathrm{sots}}, sk_{\mathrm{sots}})$. Using $sk_i$ he signs the verification key, $s_i \leftarrow \mathrm{Sign}_{sk_i}(vk_{\mathrm{sots}})$. He then creates an encryption $c$ of $(vk_i, cert_i, s_i)$ and makes a simulation-sound extractable NIZK proof $\pi$ that the plaintext is correctly formed. Finally, he makes a strong one-time signature $s_{\mathrm{sots}} \leftarrow \mathrm{Sign}_{sk_{\mathrm{sots}}}(m, vk_{\mathrm{sots}}, c, \pi)$.

The group signature on $m$ is $s = (vk_{\mathrm{sots}}, c, \pi, s_{\mathrm{sots}})$.

**Verify:** Accept if the strong one-time signature and the NIZK proof are valid.

**Open:** To open a valid group signature we decrypt $c$. We get some $(vk_*, cert_*, s_*)$ and look up the member $i$ who registered $vk_*$. In case no such member exists, we set $i = \texttt{issuer}$. We return an opening $(i, \psi)$, where $\psi = (vk_*, cert_*, s_*)$.

**Judge:** Anybody can check whether $cert_*$ is a signature on $vk_*$ under $vk$, and whether $s_*$ is a signature on $vk_{\mathrm{sots}}$ under $vk_*$. If $vk_*$ has been registered for user $i$, or no $vk_*$ has been registered and $i = \texttt{issuer}$ we accept the opening.

**Theorem 9.** *If the DLIN assumption holds for $\mathcal{G}$ then there exists a group signature scheme with anonymity, traceability and non-frameability and perfect correctness. All public keys contain $\mathcal{O}(1)$ group elements, openings contain $\mathcal{O}(1)$ group elements, and signatures contain $\mathcal{O}(1)$ group elements and elements from $\mathbb{Z}_p$.*

*Sketch of proof.* We get anonymity, because the information $(vk_i, cert_i, s_i)$ that could identify the signer is encrypted and the NIZK proof is zero-knowledge. Seeing openings of other group signatures does not help, because when a CPA-secure cryptosystem is combined with a simulation-sound proof of knowledge of the plaintext, then it becomes CCA2-secure, see also [23].

We get traceability because by the soundness of the NIZK proof system we must have a correct $(vk_*, cert_*, s_*)$ inside the ciphertext. Since only the issuer knows the signing key $ik$, nobody else can forge a certificate $cert_*$. This means, the group signature must point to some member $i$, not the issuer.

We have non-frameability because a valid signature and a valid opening pointing to $i$ contains a signature $s_*$ under $vk_i$ on $vk_{\mathrm{sots}}$, so $vk_{\mathrm{sots}}$ must have been signed by the member. Furthermore, since it is a strong one-time signature scheme and the public key $vk_{\mathrm{sots}}$ is used only once by $i$, it must also be this member that made the signature $s_{\mathrm{sots}}$ on $(m, vk_{\mathrm{sots}}, c, \pi)$.

The full paper [28] contains a more detailed construction and the full proof. □

## 6 Acknowledgment

We would like to thank Rafail Ostrovsky, Amit Sahai and Brent Waters for many discussions.

## References

1. Giuseppe Ateniese, Jan Camenisch, Susan Hohenberger, and Breno de Medeiros. Practical group signatures without random oracles. Cryptology ePrint Archive, Report 2005/385, 2005. `http://eprint.iacr.org/2005/385`.
2. Giuseppe Ateniese and Breno de Medeiros. Efficient group signatures without trapdoors. In *proceedings of ASIACRYPT '03, LNCS series, volume 2894*, pages 246–268, 2003. Revised paper available at `http://eprint.iacr.org/2002/173`.
3. Guiseppe Ateniese, Jan Camenisch, Marc Joye, and Gene Tsudik. A practical and provably secure group signature scheme. In *proceedings of CRYPTO '00, LNCS series, volume 1880*, pages 255–270, 2000.
4. Mihir Bellare, Alexandra Boldyreva, and Adriana Palacio. An uninstantiable random-oracle-model scheme for a hybrid encryption problem. In *proceedings of EUROCRYPT '04, LNCS series, volume 3027*, pages 171–188, 2004. Full paper available at `http://eprint.iacr.org/2003/077`.
5. Mihir Bellare, Daniele Micciancio, and Bogdan Warinschi. Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions. In *proceedings of EUROCRYPT '03, LNCS series, volume 2656*, pages 614–629, 2003.
6. Mihir Bellare and Phillip Rogaway. Random oracles are practical: A paradigm for designing efficient protocols. In *ACM CCS '93*, pages 62–73, 1993.
7. Mihir Bellare, Haixia Shi, and Chong Zhang. Foundations of group signatures: The case of dynamic groups. In *proceedings of CT-RSA '05, LNCS series, volume 3376*, pages 136–153, 2005.
8. Manuel Blum, Alfredo De Santis, Silvio Micali, and Giuseppe Persiano. Noninteractive zero-knowledge. *SIAM Jornal of Computation*, 20(6):1084–1118, 1991.
9. Manuel Blum, Paul Feldman, and Silvio Micali. Non-interactive zero-knowledge and its applications. In *proceedings of STOC '88*, pages 103–112, 1988.
10. Dan Boneh, Xavier Boyen, and Hovav Shacham. Short group signatures. In *proceedings of CRYPTO '04, LNCS series, volume 3152*, pages 41–55, 2004.
11. Dan Boneh, Eu-Jin Goh, and Kobbi Nissim. Evaluating 2-dnf formulas on ciphertexts. In *proceedings of TCC '05, LNCS series, volume 3378*, pages 325–341, 2005.
12. Xavier Boyen and Brent Waters. Compact group signatures without random oracles. In *proceedings of EUROCRYPT '06, LNCS series, volume 4004*, pages 427–444, 2006.
13. Jan Camenisch and Jens Groth. Group signatures: Better efficiency and new theoretical aspects. In *proceedings of SCN '04, LNCS series, volume 3352*, pages 120–133, 2004. Full paper available at `http://www.brics.dk/~jg/GroupSignFull.pdf`.
14. Jan Camenisch and Anna Lysyanskaya. Dynamic accumulators and application to efficient revocation of anonymous credentials. In *proceedings of CRYPTO '02, LNCS series, volume 2442*, pages 61–76, 2002.
15. Jan Camenisch and Anna Lysyanskaya. Signature schemes and anonymous credentials from bilinear maps. In *proceedings of CRYPTO '04, LNCS series, volume 3152*, pages 56–72, 2004.

16. Jan Camenisch and Markus Michels. A group signature scheme with improved efficiency. In *proceedings of ASIACRYPT '98, LNCS series, volume 1514*, pages 160–174, 1998.
17. Jan Camenisch and Markus Stadler. Efficient group signature schemes for large groups. In *proceedings of CRYPTO '97, LNCS series, volume 1294*, pages 410–424, 1997.
18. Ran Canetti, Oded Goldreich, and Shai Halevi. The random oracle methodology, revisited. In *proceedings of STOC '98*, pages 209–218, 1998.
19. Ran Canetti, Oded Goldreich, and Shai Halevi. On the random-oracle methodology as applied to length-restricted signature schemes, 2004.
20. Ran Canetti, Hugo Krawczyk, and Jesper Buus Nielsen. Relaxing chosen-ciphertext security. In *proceedings of CRYPTO '03, LNCS series, volume 2729*, pages 565–582, 2003. Full paper available at `http://eprint.iacr.org/2003/174`.
21. David Chaum and Eugène van Heyst. Group signatures. In *proceedings of EUROCRYPT '91, LNCS series, volume 547*, pages 257–265, 1991.
22. Alfredo De Santis, Giovanni Di Crescenzo, Rafail Ostrovsky, Giuseppe Persiano, and Amit Sahai. Robust non-interactive zero knowledge. In *proceedings of CRYPTO '01, LNCS series, volume 2139*, pages 566–598, 2002.
23. Alfredo De Santis and Giuseppe Persiano. Zero-knowledge proofs of knowledge without interaction. In *proceedings of FOCS '92*, pages 427–436, 1992.
24. Danny Dolev, Cynthia Dwork, and Moni Naor. Non-malleable cryptography. *SIAM Journal of Computing*, 30(2):391–437, 2000.
25. Uriel Feige, Dror Lapidot, and Adi Shamir. Multiple non-interactive zero knowledge proofs under general assumptions. *SIAM Journal of Computing*, 29(1):1–28, 1999.
26. Jun Furukawa and Hideki Imai. An efficient group signature scheme from bilinear maps. In *proceedings of ACISP '05, LNCS series, volume 3574*, pages 455–467, 2005.
27. Shafi Goldwasser and Yael Tauman Kalai. On the (in)security of the fiat-shamir paradigm. In *proceedings of FOCS '03*, pages 102–, 2003. Full paper available at `http://eprint.iacr.org/2003/034`.
28. Jens Groth. Simulation-sound nizk proofs for a practical language and constant size group signatures, 2006. Full paper available at `http://www.brics.dk/~jg/NIZKGroupSignFull.pdf`.
29. Jens Groth, Rafail Ostrovsky, and Amit Sahai. Non-interactive zaps and new techniques for nizk. In *proceedings of CRYPTO '06, LNCS series, volume 4117*, pages 97–111, 2006.
30. Jens Groth, Rafail Ostrovsky, and Amit Sahai. Perfect non-interactive zero-knowledge for np. In *proceedings of EUROCRYPT '06, LNCS series, volume 4004*, pages 339–358, 2006.
31. Aggelos Kiayias, Yiannis Tsiounis, and Moti Yung. Traceable signatures. In *proceedings of EUROCRYPT '04, LNCS series, volume 3027*, pages 571–589, 2004. Full paper available at `http://eprint.iacr.org/2004/007`.
32. Aggelos Kiayias and Moti Yung. Group signatures with efficient concurrent join. In *proceedings of EUROCRYPT '05, LNCS series, volume 3494*, pages 198–214, 2005. Full paper available at `http://eprint.iacr.org/345`.
33. Joe Kilian and Erez Petrank. An efficient noninteractive zero-knowledge proof system for np with general assumptions. *Journal of Cryptology*, 11(1):1–27, 1998.
34. Jesper Buus Nielsen. Separating random oracle proofs from complexity theoretic proofs: The non-committing encryption case. In *proceedings of CRYPTO '02, LNCS series, volume 2442*, pages 111–126, 2002.
35. Amit Sahai. Non-malleable non-interactive zero-knowledge and adaptive chosen-ciphertext security. In *proceedings of FOCS '01*, pages 543–553, 2001.
36. Brent Waters. Efficient identity-based encryption without random oracles. In *proceedings of EUROCRYPT '05, LNCS series, volume 3494*, pages 114–127, 2005.